

## Tinjauan Penipuan dengan Motif Pemalsuan *Barcode Qris* Dari Aspek Penanggulangan Berdasarkan Hukum Pidana Indonesia

Rindy Baruadi, Moh. Rusdiyanto U. Puluhulawa, Vifi Swarianata  
Fakulty of Law, Universitas Negeri Gorontalo, Indonesia.

Alamat : Jl. Jend. Sudirman No.6, Dulalowo Tim., Kec. Kota Tengah, Kota Gorontalo, Gorontalo 96128

E-mail korespondensi : [rindybaruadi371@gmail.com](mailto:rindybaruadi371@gmail.com)

**Abstract:** *This research aims to determine criminal acts of fraud with the motive of counterfeiting Qris Barcodes in terms of the aspect of prevention through the Indonesian Criminal Law. This research is normative research which is analyzed descriptively, using a law and case approach. The results of the research are that regulations regarding criminal acts of fraud are generally regulated in Article 378 of the Criminal Code, and to strengthen the legal basis it can be accommodated through Article 35 of Law Number 19 of 2016 concerning Information and Electronic Transactions. As a special law, the ITE Law is at least a guideline and legal basis for members of the public in carrying out activities in the online world. Overcoming the occurrence of criminal acts of online fraud is carried out with preventive (non-penal) and repressive (penal) efforts. Repressive efforts in this case are regulated based on Article 35 of the ITE Law and Article 378 of the Criminal Code. Meanwhile, preventive efforts are carried out by taking precautions so that criminal acts of online fraud can be minimized without applying criminal law, but rather by carrying out preventive efforts before the criminal act occurs, such as improving the community's economy, socializing to the public how to use the internet properly and the characteristics of electronic transaction-based criminal acts of fraud.*

**Keywords:** *Fraud; Qris Barcode; Criminal law*

**Abstract:** Penelitian ini bertujuan untuk mengetahui tindak pidana penipuan dengan motif pemalsuan Barcode Qris ditinjau dari aspek penanggulangan melalui Hukum Pidana Indonesia. Penelitian ini merupakan penelitian Normatif yang dianalisis secara deskriptif, dengan pendekatan undang-undang dan kasus. Hasil penelitian yakni Pengaturan mengenai tindak pidana penipuan secara umum diatur dalam pasal 378 KUHP, dan untuk memperkuat dasar hukum dapat diakomodir melalui Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Sebagai Undang-undang yang bersifat khusus, UU ITE setidaknya menjadi pedoman dan dasar hukum bagi anggota masyarakat dalam menjalankan aktivitas di dunia *online*. Penanggulangan terjadinya tindak pidana penipuan secara *online* dilakukan dengan upaya preventif (non penal) dan represif (penal). Upaya represif dalam hal ini diatur berdasarkan Pasal 35 UU ITE dan dalam pasal 378 KUHP. Sedangkan upaya preventif dilakukan dengan pencegahan supaya tindak pidana penipuan *online* dapat diminimalkan tanpa melalui penerapan hukum pidana melainkan dilakukannya upaya pencegahan sebelum terjadinya tindak pidana itu, seperti memperbaiki perekonomian masyarakat, mensosialisasikan kepada masyarakat bagaimana penggunaan internet yang baik serta bagaimana ciri tindak pidana penipuan berbasis transaksi elektronik.

**Kata Kunci:** Penipuan; Barcode Qris; Hukum Pidana

### PENDAHULUAN

Perubahan rutinitas sosial-ekonomi masyarakat adalah salah satu contoh percepatan tersebut. Sebelumnya, hanya pertemuan di tempat-tempat seperti pasar, toko, supermarket, atau mall yang digunakan untuk kegiatan bisnis dan transaksional. Namun, berkat revolusi teknologi saat ini, masyarakat kini memiliki pilihan untuk melakukan aktivitas virtual melalui layar, gawai, atau komputer.

Peningkatan inovasi untuk membantu perubahan kegiatan moneter dari biasa menjadi virtual telah dibuktikan melalui hadirnya pembayaran non tunai (*cash less*) yang dapat bekerja

sama dengan bursa baik secara lokal maupun universal. Menurut data Bank Indonesia tahun 2019, uang elektronik memimpin pembayaran nontunai dengan transaksi 95,75 triliun, naik dari 60,00 triliun pada tahun sebelumnya (2018). Uang elektronik banyak digunakan untuk pembayaran nontunai sebagai akibat dari perkembangan produk uang elektronik, yang meliputi kartu *e-money* berbasis *chip* dan *server*, serta aplikasi *e-wallet* dan rekening bank. Kenyamanan yang disajikan melalui pertukaran uang virtual secara positif berdampak besar. Ini mungkin karena industri teknologi keuangan yang berkembang, yang dimulai oleh banyak bisnis baru dan mengarah ke berbagai dompet digital untuk menyimpan uang elektronik seperti ShopeePay dari Shopee, Go-Pay dari Go-Jek, Ovo, DANA, LinkAja, dan lainnya.

Tugas inovasi data dan korespondensi di era globalisasi telah menempatkannya pada posisi yang sangat esensial karena menghadirkan dunia tanpa batas, jarak, realitas, yang berdampak pada peningkatan efisiensi dan kecakapan. Gaya hidup masyarakat telah berubah sebagai akibat dari globalisasi dan penggunaan teknologi informasi dan komunikasi, lebih jauh lagi, menciptakan tuntutan hidup yang lain dan pemberdayaan sosial, moneter, budaya, perlindungan, keamanan dan penegakan hukum. Teknologi informasi dan komunikasi dewasa ini digunakan dalam kehidupan sosial masyarakat dan telah memasuki berbagai bidang lainnya, antara lain perbankan, pendidikan, kesehatan, kehidupan pribadi, dan sektor pemerintahan. “Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga didasari memberi peluang untuk dijadikan sarana melakukan tindak kejahatan-kejahatan baru (*cybercrime*) sehingga diperlukan upaya proteksi.” Jadi bisa dikatakan bahwa inovasi data dan korespondensi menyerupai kesepakatan dua sisi, yang selain membuat komitmen positif untuk memperluas bantuan, kemajuan dan pembangunan pemerintah manusia, juga merupakan metode yang potensial dan memaksa untuk melakukan tindakan ilegal.

Aktivitas yang sah di internet adalah keanehan yang sangat menegangkan, mengingat pengecekan, peretasan, pemerasan, penindasan psikologis, dan penyebaran data yang menghebohkan telah menjadi bagian dari aktivitas pelaku kejahatan di internet. Hal ini sangat kontras dengan kurangnya peraturan yang mengatur penerapan teknologi informasi dan komunikasi di berbagai industri “Oleh regulasi terhadap berbagai aktivitas terkait dengan pemanfaatan teknologi informasi dan komunikasi tersebut”.

Isu unjuk rasa kriminal merupakan keanehan sosial yang umumnya menjadi bahan pertimbangan berbagai kalangan, khususnya para pelaksana regulasi. Demonstrasi kriminal tidak dapat dibedakan dari siklus keuangan yang sedang berjalan dan pola serta mengarahkan

jenis perilaku setiap penduduk. Di mana salah satu dinamika sosial yang menjadi landasan terjadinya perbuatan jahat atau kejahatan.

Salah satu bentuk kejahatan yang sangat wajar di mata publik adalah penipuan. Penipuan dapat dilakukan hanya dengan memiliki kemampuan relasional yang baik sehingga seseorang dapat meyakinkan orang lain, baik melalui serangkaian kebohongan atau kata-kata imajiner. Sekarang ini ada banyak demonstrasi kriminal penipuan, bahkan mereka maju dengan menyenangkan dalam struktur yang berbeda. Kemajuan ini menunjukkan semakin tingginya tingkat pendidikan para pelaku penipuan yang semakin kompleks, salah satunya adalah pembuatan *scanner tag*. Mengingat sejarahnya, bisnis ritel adalah yang pertama menggunakan teknologi *barcode*, diikuti oleh bisnis industri. Pada tahun 1932, Wallace Flint menciptakan sistem ini, yang digunakan untuk mengecek barang dagangan di bisnis retail. *Barcode* dapat diibaratkan sebagai kumpulan kode-kode yang berbentuk garis-garis, dengan ketebalan tiap garis berbeda-beda tergantung dari isi kode tersebut. Demikianlah pengertian dari *barcode* dapat diartikan.

Melihat hal tersebut maka badan publik mengatur dan menetapkan pedoman terkait dengan *barcode* ini agar tidak terjadi penyalahgunaan informasi terhadap informasi perseorangan yang tertuang dalam peraturan Pemerintah Republik Indonesia No 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik Pasal 1 ayat 23. Selain terdapat dalam peraturan pemerintah, *barcode* juga diatur dalam Peraturan Anggota Dewan Gubernur Nomor 21/18/PADG/2019 Tentang Implementasi Standar Nasional *Quick Response Code* untuk pembayaran.

Adapun sesuai dengan pembahasan diatas mengenai identifikasi *barcode* yang menjadi suatu sistem yang digunakan untuk mempermudah dalam bertransaksi, yang pengaturannya diatur dalam Peraturan Anggota Dewan Gubernur No 21/18/PADG/2019 yang pada pasal 1 ayat 4 ada pemahaman “*Quick Response (QR) Code* untuk Pembayaran adalah kode dua dimensi yang terdiri atas penanda tiga pola persegi pada sudut kiri bawah, sudut kiri atas, dan sudut kanan atas, memiliki kemampuan menyimpan data alfanumerik, karakter, dan simbol, yang digunakan untuk memfasilitasi transaksi pembayaran di Indonesia.” Selain itu, pengertian Standar Pembayaran *QR Code* Nasional (*Quick Response Code Indonesian Standard*) dapat dilihat pada ayat 5. Standar *QR Code* pembayaran ini ditetapkan oleh Bank Indonesia dengan maksud untuk memudahkan dalam melakukan pembayaran di Indonesia. Ruang lingkup QRIS juga telah diatur dalam pasal 2, khususnya pada ayat 1: “*QR Code* Pembayaran Memiliki fungsi utama untuk menampilkan identitas salah satu pihak dalam pemrosesan transaksi pembayaran.” Dan pada ayat 2 dari pasal 2 mengatakan “Dalam pemrosesan transaksi

pembayaran, *QR Code* pembayaran ditampilkan oleh salah satu pihak yang bertransaksi untuk kemudian dipindai oleh pihak lainnya.”

Konsep penipuan (*bedrod*) yang terdapat dalam pasal 378 KUHP merupakan tindak pidana atau delik, apabila diabaikan akan tergantung pada sanksi penjara. Masih terdapat berbagai macam pendapat dan pemaknaan terhadap istilah delik, Leden marpaung memberi istilah “delik atau “*strafbaar feit*”(bahasa Belanda),”*delictum*”(bahasa Latin),”*criminal act*”(bahasa Inggris) yang berarti perbuatan yang dilarang oleh peraturan hukum pidana dan mendapat sanksi pidana bagi barang siapa yang melanggarnya”.

Dilihat dari kondisi yang terjadi di masyarakat saat ini, dapat memunculkan permasalahan yang berbeda dalam penyelesaian demonstrasi kriminal di bidang inovasi data. Keterusterangan yang dapat digunakan seseorang untuk menggunakan karakter apa pun untuk melakukan berbagai jenis pertukaran elektronik di mana saja dapat mempersulit kepolisian untuk mengidentifikasi karakter asli dan lokasi pelakunya. Mengingat ketentuan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, keberadaan bukti elektronik yang dapat diterima sebagai alat bukti yang sah akan menjadi topik yang signifikan di tahun-tahun mendatang. Berkembangnya inovasi data termasuk web juga memberikan kesulitan tersendiri bagi kemajuan regulasi di Indonesia.

Di Indonesia, hukum harus mampu beradaptasi dengan perubahan sosial. Perubahan sosial dan perubahan hukum atau sebaliknya tidak selalu terjadi secara bersamaan. Artinya pada keadaan tertentu perkembangan hukum mungkin tertinggal oleh perkembangan unsur-unsur lainnya dari masyarakat serta kebudayaannya atau mungkin hal yang sebaliknya. Hal ini dapat kita lihat dari keuntungan hadirnya QRIS yang semakin memudahkan dalam hal transaksi pembayaran dan beramal, namun masih ada saja penyalahgunaan yang dilakukan oleh pihak-pihak yang ingin mendapatkan keuntungan sesaat. Penyalahgunaan ini adalah tindak pidana penipuan dengan alasan memalsukan identifikasi standar QRIS. Salah satunya adalah yang dilakukan oleh seorang pria yang menempelkan QRIS di kotak amal sebuah masjid di Blok M Square. Tindakan pria itu terekam oleh kamera CCTV, dan akhirnya dibagikan secara luas di media sosial. Kelompok masyarakat melihat kegiatan ini sebagai bentuk lain dari pengambilan kotak amal masjid. Adapun hal yang dilakukan oleh pelaku adalah stiker kotak amal atau infak resmi yang berbasis QRIS diganti pelaku dengan stiker kotak amal palsu yang dilengkapi dengan *QR Code* seperti halnya QRIS. Akan tetapi, nomor rekening yang terhubung dengan QRIS palsu tersebut bukan rekening masjid melainkan ke rekening pribadi pelaku.

*Cybercrime* adalah jenis kejahatan yang muncul sebagai akibat dari penggunaan

teknologi internet. Kejahatan didorong oleh pesatnya pertumbuhan penggunaan layanan internet. Mengikuti perkembangan teknologi itu sendiri, kejahatan yang dilakukan terhadap pengguna teknologi informasi semakin meningkat seiring dengan meningkatnya jumlah permintaan akses internet. Jika tidak ada undang-undang yang mengatur kejahatan dunia maya ini, tindakan para pelakunya semakin merugikan banyak pihak. Sebelum berlakunya undang-undang ITE, pihak berwenang menangani kasus kejahatan dunia maya dengan menggunakan KUHP.

Berdasarkan uraian di atas, ternyata perkembangan ilmu pengetahuan dan teknologi yang pesat selalu diikuti atau diiringi dengan perkembangan kejahatan atau tindak pidana yang makin canggih dan maju pula. Hal ini ditandai dengan pesatnya perkembangan cara melakukan modus operan maupun alat yang digunakannya.

## **METODE PENELITIAN**

Metode yang digunakan dalam penelitian ini ialah normative, yang meletakkan hukum sebagai sebuah bangunan sistem norma. Sistem norma yang dimaksud adalah mengenai asas-asas, norma, kaidah dari peraturan perundang-perundangan, putusan pengadilan, perjanjian serta doktrin (ajaran).

## **HASIL DAN PEMBAHASAN**

Upaya preventif lebih menekankan pada pencegahan sebelum terjadinya tindak pidana atau hal-hal yang dilakukan sebelum terjadinya suatu tindak pidana. Pencegahan dilakukan dengan sosialisasi atau pemberitaan melalui media dan juga koordinasi antar lembaga dalam merumuskan rangka penegakan Undang-undang, atau membuat media sebagai sarana untuk masyarakat mengetahui lebih lanjut tentang hukum di ITE. Media yang digunakan sebagai sarana informasi ini dapat menjadi media pembelajaran masyarakat supaya tidak mudah ditipu secara *online*.

Upaya lain berupa upaya represif, dimana lebih menekankan pada tindakan yang dilakukan penegak hukum setelah terjadi suatu tindak pidana. Upaya represif dilakukan dengan menindaklanjuti laporan terkait tindak pidana yang termasuk pada penipuan *online*, kemudian memberikan sanksi hukum yang tegas terhadap pelaku sesuai dengan pasal terkait guna memberikan efek jera dan sesuai dengan rasa keadilan didalam masyarakat.

Kebijakan hukum pidana adalah penerapan hukum pidana untuk menanggulangi kejahatan. Pengertian hukum pidana sama dengan kebijakan *penal policy*, sehingga pengertian kebijakan hukum pidana terhadap *cybercrime* adalah penerapan hukum pidana untuk menanggulangi *cybercrime*. Marc Ancel pernah menyatakan, bahwa “*modern criminal science*” terdiri dari tiga komponen yaitu “*criminology*”, “*criminal law*”, dan “*penal policy*”. Dikemukakan olehnya, bahwa *penal policy* adalah suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak hanya kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada para penyelenggara atau pelaksana putusan pengadilan.

Kebijakan penal (kebijakan hukum pidana) adalah penanggulangan kejahatan dengan menggunakan hukum pidana (*criminal law application*). Kebijakan tersebut di operasionalisasikan dengan cara menerapkan hukum pidana, yaitu hukum materiil, hukum formil, dan hukum penitensier dalam masyarakat. Operasionalisasi kebijakan hukum

penal meliputi kriminalisasi, diskriminalisasi, penalisasi, dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial, oleh karena itu penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu perilaku social.

Upaya penanggulangan kejahatan dengan hukum pidana pada hakikatnya juga merupakan bagian dari usaha penegakan hukum, oleh karena itu sering pula dikatakan bahwa politik atau kebijakan hukum pidana merupakan bagian dari kebijakan penegakan hukum (*law enforcement policy*). Di samping itu, upaya penanggulanngan kejahatan lewat pembuatan undang-undang (hukum) pidana pada hakikatnya juga merupakan bagian integral dari usaha perlindungan masyarakat (*social welfare*).

Hoefnegels mengemukakan bahwa penerapan hukum pidana untuk menanggulangi kejahatan meliputi ruang lingkup sebagai berikut :

- a) Administrasi peradilan pidana dalam arti sempit, yaitu pembuatan hukum pidana dan yurisprudensi, proses peradilan pidana dalam arti luas meliputi ilmu kejiwaan, ilmu social, dan pembedanaan.
- b) Psikiatri dan psikologi forensik.
- c) Forensik kerja social.
- d) Kejahatan, pelaksanaan pembedanaan dan kebijakan statistik.

Kebijakan hukum pidana dapat didefinisikan sebagai usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada sewaktu waktu dan untuk masa yang akan datang.

A. mulder mengemukakan bahwa kebijakan hukum pidana ialah kebijakan untuk menentukan :

- a) Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu di rubah atau di perbarui;
- b) Apa yang dapat di perbuat untuk mencegah terjadinya tindak pidana
- c) Cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan.

Pada hakekatnya kebijakan untuk membuat peraturan hukum pidana menjadi lebih baik merupakan bagian dari upaya dalam penanggulangan kejahatan. Dengan demikian kebijakan hukum pidana hakekatnya merupakan bagian dari kebijakan penaggulangan kejahatan (politik kriminal). Berkaitan dengan penerapan dalam hukum pidana *criminal policy*, Bambang Purnomo berpendapat, bahwa tujuan hukum pidana adalah masyarakat dan setiap anggota masyarakat terlindung dari hukum sehingga mencapai kesejahteraan lahir batin. Tujuan ini tidak lepas dari fungsi hukum pidana, yaitu: fungsi primer, sebagai sarana untuk mencegah kejahatan.

Fungsi sekunder hukum pidana yakni menindak pelaku kejahatan fungsi sekunder di terapkan jika fungsi primer tidak mampu dilaksanakan. Dalam lingkup kebijakan penanggulangan kejahatan, hukum pidana hanya merupakan salah satu upaya dari beberapa upaya penanggulangan kejahatan. Terkait dengan masalah kebijakan penanggulangan tindak pidana menurut uladi terdapat dua masalah sentral dalam kebijakan kriminal dengan menggunakan sarana penal (hukum pidana ) ialah masalah penentuan

- a) Perbuatan apa yang harusnya di jadikan tindak pidana dan
- b) Sanksi apa yang sebaiknya di gunakan atau di kenakan kepada si pelanggar.

Pemberian sanksi dalam kebijakan hukum pidana, maka terlebih dahulu harus mengetahui seluk beluk hakikat suatu sanksi hukum. Sanksi hukum adalah sanksi atau hukuman yang di jatuhkan pada seseorang yang melanggar hukum. Sanksi hukum diatur oleh hukum baik mengenai ruang lingkup maupun cara pelaksanaannya. Sanksi diadakan sebagai kosekuensi dari perbuatan yang di anggap merugikan masyarakat dan yang menurut tata hukum terus dihindari. perbuatan yang merugikan ini disebut delik. Sanksi yang diberikan tata hukum dengan maksud untuk menimbulkan perbuatan tertentu yang dikehendaki oleh pembuat undang-undang. Pelanggaran terhadap norma hukum akan berakibat adanya sanksi hukuman

yang sifatnya memaksa, yaitu hukuman mati, hukuman penjara atau kurungan dan hukuman denda.

Dengan demikian dapat ditegaskan, bahwa masalah sentral hukum pidana mencakup tindak pidana, pertanggungjawaban pidana dan pidana. Kebijakan hukum pidana termasuk kebijakan dalam menanggulangi dua masalah sentral tersebut, yang harus dilakukan dengan pendekatan yang berorientasi pada kebijakan (*policy oriented approach*) sehingga kebijakan hukum pidana (*penal policy*) dapat didefinisikan sebagai usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang. Definisi tersebut sekilas terlihat bahwa kebijakan hukum pidana identik dengan pembaharuan perundang-undangan hukum pidana namun sebenarnya antara keduanya berbeda, dimana hukum pidana sebagai suatu sistem hukum yang terdiri dari budaya (*culture*), struktur dan substansi hukum, sehingga pembaharuan hukum pidana tidak sekedar memperbaharui perundang-undangan hukum pidana saja namun juga memperbaiki sektor-sektor lain seperti ilmu hukum pidana dan ide-ide hukum pidana melalui proses Pendidikan dan pemikiran akademik.

Upaya penanggulangan melalui kebijakan hukum pidana dilaksanakan melalui kriminalisasi hukum pidana yaitu dengan pembentukan undang-undang yang secara khusus mengatur perbuatan yang dilarang tersebut. Upaya penanggulangan tindak pidana siber (*cybercrime*) melalui sarana penal tercantum dalam Undang-undang Nomor 19 Tahun 2016 tentang perubahan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Upaya penanggulangan tindak pidana penipuan yang dilakukan secara online melalui sarana penal diatur pada Pasal 35 Undang-undang Informasi dan Transaksi Elektronik. Melakukan manipulasi, penciptaan, perubahan, penghilangan dan pengrusakan informasi elektronik merupakan padanan kata yang semakna dengan penipuan. Penipuan dapat dilakukan dengan motivasi, yaitu untuk menguntungkan dirinya dan merugikan orang lain secara sekaligus. Dengan motivasi-motivasi tersebut, maka dengan melakukan manipulasi, penciptaan, perubahan, penghilangan dan pengrusakan informasi elektronik dapat dikategorikan sebagai penipuan. Secara umum penipuan itu telah diatur sebagai tindak pidana dalam Pasal 378 Kitab Undang-undang Hukum pidana.

Perbuatan yang dikriminalisasi dalam pasal 35 Undang-undang Informasi dan Transaksi Elektronik sebagai bentuk upaya penanggulangan tindak pidana penipuan tersebut yaitu mengatur perbuatan dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan,

perubahan, penghilangan dan pengrusakan informasi elektronik yang mengakibatkan kerugian kepada pihak lain dalam transaksi elektronik. Pelanggaran terhadap ketentuan Pasal 35 diancam dengan Pasal 51 ayat (1) yaitu dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak dua belas miliar rupiah miliar rupiah.

Kebijakan perundang-undangan secara fungsional dapat dilihat sebagai bagian dari perencanaan dan mekanisme penanggulangan kejahatan bahkan dapat dikatakan sebagai langkah awal. Penggunaan hukum pidana pada upaya pencegahan dan penanggulangan *cybercrime* sangat relevan mengingat bahaya-bahaya dan kerugian yang ditimbulkan dari meningkat pesatnya teknologi informasi tersebut menjadi pertimbangan yang sangat layak. Hukum pidana dipanggil untuk menyelamatkan kerugian yang diderita oleh masyarakat karena kejahatan tersebut dapat menghalangi aktifitas kehidupan sosial-ekonomi masyarakat.

Sehingga sebagai bentuk upaya penanggulangan tindak pidana penipuan berbasis transaksi elektronik dan informasi elektronik dalam mencapai perlindungan terhadap kepentingan masyarakat (*social defence*) tersebut, maka keberadaan hukum pidana sangat diperlukan agar dapat teratasinya kejahatan di dunia siber yang notabenenya menjadi penghambat pembangunan kesejahteraan masyarakat, upaya melalui kebijakan hukum pidana yang integral harus dimaksimalkan. Melalui dari substansi hukum, struktur hukum bahkan kultur hukumnya harus berjalan dengan maksimal. Hanya melalui penegakan hukum pidana yang terpadu diharapkan fungsionalisasi hukum pidana dalam penanggulangan tindak pidana penipuan berbasis transaksi elektronik dapat terealisasikan.

Kebijakan lain sebagai upaya penanggulangan terjadinya tindak pidana penipuan *online* yaitu melalui kebijakan non penal. Kebijakan ini lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan. Barda Nawawi menjelaskan bahwa untuk mencegah suatu tindak pidana kejahatan, maka sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan. Faktor-faktor itu antara lain, berpusat pada masalah-masalah atau kondisi-kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuhkan kejahatan. Dengan demikian dilihat dari sudut politik kriminal, maka upaya pencegahan menduduki posisi kunci dan strategi dari keseluruhan upaya politik kriminal (Barda Nawawi Arief, 2007:46).

Kebijakan non penal dapat ditempuh dengan memperbaiki perekonomian nasional, melakukan pendidikan budi pekerti kepada setiap orang baik secara formal maupun informal khususnya kepada pihak yang cenderung terdorong untuk melakukan kejahatan. Kemudian dengan memperbaiki sistem kesehatan mental masyarakat, mengefektifkan kerjasama internasional dalam pemberantasan kejahatan siber, memperbaiki sistem keamanan komputer

dan teknologi informasi, serta melakukan efektivitas terhadap hukum administrasi dan hukum perdata yang berhubungan dengan penyelenggaraan sistem dan jaringan internet (Widodo,2011:191).

Perkembangan internet membuka akses seluas-luasnya bagi semua pihak untuk dapat memanfaatkan teknologi informasi dan komunikasi tersebut dengan murah dan cepat. Disisi lain, keberadaan internet sebagai sarana baru penunjang aktifitas tersebut memberikan dampak negatif kepada para penggunanya untuk melakukan kejahatan baru.

Upaya penanggulangan tindak pidana melalui sarana non penal dianggap strategis dalam menanggulangi sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan, hal ini ditegaskan dalam berbagai Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders*. Pada kongres PBB ke-6 Tahun 1980 di Caracas Venezuela, dinyatakan didalam pertimbangan resolusi mengenai *crime tends and crime prevention strategies*, antara lain sebagai berikut:

- a) Bahwa masalah kejahatan merintangki kemajuan untuk pencapaian kualitas lingkungan hidup yang layak/pantas bagi semua orang.
- b) Bahwa strategi pencegahan kejahatan harus didasarkan pada penghapusan sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan.
- c) Bahwa penyebab utama dari kejahatan di banyak negara ialah kepentingan social, diskriminasi rasial, dan diskriminasi nasioanl, standar hidup yang rendah, pengangguran dan kebodohan diantara golongan besar penduduk,

Hal menarik dari kebijakan non penal yang dikemukakan dalam kongres PBB ialah upaya mengembangkan pengamanan/perlindungan computer dan tindakan-tindakan pencegahan. Jelas hal ini terkait dengan pendekatan *techno prevention*, yaitu upaya pencegahan/penanggulangan kejahatan dengan menggunakan teknologi. Sangat disadari oleh kongres PBB, bahwa *cybercrime* yang terkait erat dengan kemajuan teknologi, tidak dapat semata-mata ditanggulangi dengan pendekatan yuridis, tetapi juga harus ditanggulangi dengan pendekatan teknologi sendiri. Aspek lain yang menarik dari kebijakan non penal yang terungkap dari kongres PBB ialah perlunya pendekatan budaya, kultural dan etik dalam kebijakan penanggulangan tindak pidana siber (*cybercrime*), yaitu membangun/membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah tindak pidana siber dan menyebarluaskan/mengajarkan etika penggunaan komputer melalui pendidikan dan pendekatan budaya.

Hal ini senada dengan ketentuan dalam *Convention on Cybercrime*, bahwa kerjasama internasional yang perlu dilakukan dalam rangka penanggulangan *cybercrime* adalah perjanjian ekstradisi, mutual *assistance in criminal matters*, pemberian informasi secara spontan, dan pembentukan jaringan yang dikelola oleh tenaga-tenaga profesional dalam rangka menjamin terselenggaranya bantuan secepatnya untuk investigasi dan peradilan untuk pengumpulan alat bukti elektronik. Bantuan-bantuan tersebut meliputi pula pemberian fasilitas atau bantuan lain, dengan syarat diijinkan oleh hukum nasional masing-masing negara, dalam hal ini diatur pula tentang pertanggungjawaban korporasi (*corporate liability*), baik dalam hukum pidana maupun hukum perdata dan hukum administrasi.

Muladi berpendapat bahwa dalam kaitannya dengan upaya memerangi *cybercrime* melalui sarana non penal, memerlukan upaya sebagai berikut:

- 1) Perlu dirumuskan terlebih dahulu model undang-undang payung (*umbrella act*) yang mengatur kebijakan tentang komunikasi masa baik berbentuk cetak, penyiaran maupun siber.
- 2) Perlu dirumuskan secara professional penyusunan kode etik, *code of conduct and code of partice* tentang penggunaan teknologi informatika.
- 3) Perlu kerjasama antara pihak-pihak yang terkait termasuk kalangan industri untuk mengembangkan *preventive technology* menghadapi tindak pidana siber.

Dalam kebijakan non penal, Muladi menyatakan bahwa perlu dilakukan upaya lain dalam penanggulangan tindak pidana siber yaitu sebagai berikut:

1) Kerjasama Internasional

Sifat tindak pidana siber adalah internasional, karena itu diperlakukan kerjasama internasional yang intensif baik dalam penegakan hukum pidana maupun dalam bidang teknologi berupa pembentukan jaringan informasi yang kuat, pelatihan personil penegakan hukum yang memadai, harmonisasi hukum dan penyebarluasan kesepakatan- kesepakatan internasional. penyelarasan hukum pidana materil yang mengatur tentang tindak pidana siber merupakan inti dari kerjasama internasional, yang diharapkan diperoleh dari penegakan hukum dan kewenangan pengadilan dari negara berbeda

2) Rencana aksi Nasional Inational action plan di Indonesia

Dalam ruang lingkup nasional perlu disusun suatu rencana aksi nasional (*national acton plan*) untuk menanggulangi tindak pidana siber, karena proses viktimisasi kejahatan tersebut sangat luas dan sifatnya transional. Pemerintah dan beberapa komunitas teknologi informasi perlu menggalang kerjasama guna menanggulangi

kejahatan didunia maya (*cybercrime*). Kegiatan yang sudah dilakukan tersebut dilakukan misalnya melalui pendirian Indonesian Forum on *Information for Infocom Incident Response and Security Team* (ID-FIRST), yang diharapkan menciptakan sinergi antara pemerintah, kepolisian dan industri teknologi informasi dalam mencegah kejahatan dunia maya melalui internet.

Selain hal tersebut diatas, dalam upaya non penal yang dilakukan sebagai langkah pencegahan terhadap tindak pidana penipuan berbasis transaksi elektronik juga dapat dilakukan sebagai berikut :

1) Pendekatan Teknologi (*Techno Prevention*)

Menurut Volodymyr Golube, banyak aspek aspek dari kasus-kasus *cybercrime* yang terjadi akibat lemahnya perlindungan informasi daripada diakibatkan oleh perbuatan pelaku kejahatan. Oleh karena itu, diperlukan lebih banyak informasi mengenai kelemahan/kerentanan dari system komputer dan sarana perlindungan yang efektif. Dalam konteks *cybercrime* erat hubungannya dengan teknologi, khususnya teknologi computer dan telekomunikasi sehingga pencegahan *cybercrime* dapat digunakan melalui saluran teknologi seperti media massa dan pers (*techno prevention*).

2) Pendekatan Budaya

Pentingnya pendekatan budaya dalam kebijakan penanggulangan *cybercrime*, untuk/membangun membangkitkan kepekaan warga masyarakat dan aparat penegakan hukum terhadap masalah *cybercrime* dan menyebarluaskan atau mengajarkan etika menggunakan komputer melalui media Pendidikan. Pendekatan budaya berupa untuk mengembangkan kode etik dan perilaku khususnya upaya-upaya mengembangkan kode etik dan perilaku (*codes of behavior and ethics*) terungkap pada pernyataan IIC (*International Information Industry Conggres*) yaitu berupaya untuk membangun atau mengembangkan kode etik dan perilaku dalam menggunakan komputer dan internet dan menekankan perilaku yang etis dan bertanggung jawab serta standar norma dalam berperilaku yang berkualitas tinggi (terpuji) di ruang siber.

Upaya penanggulangan tindak pidana penipuan *online* dalam perkembangannya telah dibangun melalui sistem infrastruktur yang dibentuk melalui badan yang mengawasi lalu lintas data yaitu IdSIRTII/CC atau *Indonesian Security Incident Response Team on Internet and Infrastructure/Coordination Center* yang bertugas melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Lembaga tersebut memiliki tugas pokok untuk melakukan sosialisasi terkait keamanan IT, melakukan pemantauan dini, pendeteksian dini,

peringatan dini terhadap ancaman jaringan telekomunikasi dari dalam maupun luar negeri khususnya tindakan pengamanan pemanfaatan jaringan, membuat/menjalankan/mengembangkan dan *database log file* serta statistik keamanan internet.

Selain dari Id-SIRTII/CC, Kepolisian Republik Indonesia juga memiliki divisi yang menangani terkait kejahatan siber. Namun, anggota tim *cybercrime* dari Polri belum menyeluruh hingga ke pelosok wilayah Indonesia, melainkan baru terpusat di beberapa kota besar di Indonesia. Peran serta dari masyarakat sendiri sangat diperlukan dalam menangani serangan kejahatan siber ini, terlebih pada serangan penipuan berbasis internet. Terdapat beberapa tindakan yang mampu dilakukan untuk mencegah serangan penipuan berbasis internet yaitu:

- a. Meningkatkan *awareness* (kesadaran) organisasi tentang ancaman siber;
- b. Menerapkan standar keamanan informasi siber keseluruhan organisasi;
- c. Melatih SDM menguasai keahlian pengamanan siber secara berkelanjutan;
- d. Menerapkan arsitektur sistem dan layanan yang aman dan update periodik;
- e. Memiliki kemampuan pencegahan, mitigasi dan remediasi serta audit.

Kementrian komunikasi dan informatika tiap tahun selalu mengadakan kegiatan, dan pelatihan untuk meningkatkan kesadaran dari masyarakat terhadap pengguna internet bahwa data yang mereka masukan itu memiliki nilai, tergantung dari situasi dan kondisi. Kementrian komunikasi dan informatika sendiri telah melakukan bentuk perlindungan kepada pengguna internet Indonesia dari kejahatan siber termasuk didalamnya penipuan berbasis internet.

## **KESIMPULAN**

Pengaturan mengenai tindak pidana penipuan secara umum diatur dalam pasal 378 KUHP, dan untuk memperkuat dasar hukum dapat diakomodir melalui Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Sebagai Undang-undang yang bersifat khusus, UU ITE setidaknya menjadi pedoman dan dasar hukum bagi anggota masyarakat dalam menjalankan aktivitas di dunia *online*. Penanggulangan terjadinya tindak pidana penipuan secara *online* dilakukan dengan upaya preventif (non penal) dan represif (penal). Upaya represif dalam hal ini diatur berdasarkan Pasal 35 UU ITE dan dalam pasal 378 KUHP. Sedangkan upaya preventif dilakukan dengan pencegahan supaya tindak pidana penipuan *online* dapat diminimalkan tanpa melalui penerapan hukum pidana melainkan dilakukannya upaya pencegahan sebelum terjadinya tindak pidana itu, seperti memperbaiki

perekonomian masyarakat, mensosialisasikan kepada masyarakat bagaimana penggunaan internet yang baik serta ciri tindak pidana tersebut.

#### **DAFTAR PUSTAKA**

- , *Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP baru)*
- Abdul Wahid dan Muhammad Labib, *Kejahatan Mayantara (cybercrime)*, (Refika Aditama, 2009)
- Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*
- Budi Suhaiyanto, *Tindak pidana Teknologi Informasi (Cybercrime)*, (Jakarta: Rajawali Perss, 2013)
- Claressia S. Wibisono & Anajeng Esri Edhi Mahanani S.H,M.H., *Analisis Yuridis Terhadap Tindak Pidana Penipuan Dalam Transaksi Elektronik Melalui Media Sosial*, Vol.2 No.2, Juni 2023.
- [https://www.academia.edu/38989458/Jurnal\\_Barcode\\_dan\\_Sejarahinya?auto=download](https://www.academia.edu/38989458/Jurnal_Barcode_dan_Sejarahinya?auto=download)
- Josef Evan Sihalo, et.al, Implementasi Sistem Pembayaran Quick Response Indonesia Standar Bagi Perkembangan UMKM di Medan, *Jurnal Manajemen Bisnis*, Vol.17. No.2, April 2020.
- Leden Merpaung, 2006, *Asas Teori Praktik Hukum Pidana*, Jakarta, Sinar Grafika
- Mukti, Fajar., & Yulianto, Achmad. 2010. *Dualisme Penelitian Hukum Normatif & Empiris*. Yogyakarta: Pustaka Pelajar.
- Okky Van Royan, *Penerapan Sanksi Pidana Terhadap Tindak Pidana Penipuan Jual Beli Online Menurut Hukum Positif Indonesia*, skripsi pada Universitas Muhammadiyah Palembang, 2022
- Siswanto Sunarso, 2009, *Hukum Informasi dan Transaksi Elektronik*, Jakarta, Rineka Cipta
- Widodo, *Memerangi Cybercrime (Karakteristik, Motivasi dan Strategi Dalam Penanganannya dalam Perspektif Kriminologi)*